REMARKS/ARGUMENTS

Favorable reconsideration of this application, as presently amended and in light of the following discussion, is respectfully requested.

Claims 37-45 are pending in this application. Claims 37, 39 and 41 are amended. Support for the changes to the claims is found in the originally filed disclosure, including the original claims, the drawings at least in Fig. 26 (i.e. ST303) and the specification at least at page 80, lines 4-8. No new matter is added.

In the outstanding Office Action, Claims 37-45 were rejected under 35 U.S.C. § 112, first and second paragraphs; and Claims 37-45 were rejected under 35 U.S.C. § 103(a) as unpatentable over EP 1069567 (Asano) in view of U.S. 6,697,948 (Rabin).

Initially, regarding the rejections under 35 U.S.C. § 112, first and second paragraphs, the Office Action alleges the specification does not describe a plurality of different signatures being created using *only a single* secret key and message,[1] and further that it is unclear to one of ordinary skill how multiple different signatures can be produced when both the data being signed and a key used to generate the signature are the same.[2] Although Applicant disagrees with the Office's position regarding this issue, the claims are amended to overcome the Office's interpretation of the claims, and thus, the rejections under 35 U.S.C. §112, first and second paragraphs.

In particular, the independent claims are amended to recite, *inter alia*, different signature data elements are generated from a secret key data element, a message data element, and *a variable*. In a non-limiting example of the claimed invention, such a variable can be a random number, as identified in item 6 of the Office Action.[3] As a result of these

---

[1] Office Action, items 9 and 12, pages 3-4.
[2] Office Action, item 12, page 4.
[3] Office Action, item 6, page 3, citing paragraphs 167-174 of Applicant's specification as published.

amendments, it is respectfully submitted the rejections under 35 U.S.C. § 112, first and second paragraphs, are overcome and should be withdrawn.

As to the cited references, the Office Action acknowledges Asano fails to disclose or reasonably suggest producing a plurality of different signature elements and including one of the elements in identification data, where the identification data includes a message data element, which was used in the generation of the plurality of different signature data elements. For this feature, the Office Action relies on Rabin.

Rabin describes a process of assigning a unique number to an instance of named software and computing a hash of the software.[4] A hash value for the instance is also created, where this 'instance hash' is a variable of a name of the software, the assigned unique number, and the computed hash of the software.[5] Then a signed tag for the software is created, which includes the name of the software, the unique number assigned thereto, the hash of the instance and a signed hash of the instance. In an alternative arrangement shown in Figure 3B, the hash of the instance is not signed, and is thus not included in the tag for the software.[6]

It appears the hash of the instance is relied upon as the claimed message data element and the signature data element is the signed version of the hash of the instance. However, as noted above, the hash of the instance is a hash of the name of the software, the unique number and a hash of the software itself. To the contrary, as amended, Claim 37 requires the message data to be a generator of a cyclic group for a title of encrypted content. Since the feature relied upon in Rabin is a hash of several variables, including a hash of software, the unique number, and a name of the software, it is respectfully submitted the relied upon message data in Rabin is not a generator of a cyclic group for a title of an encrypted content.

---

[4] Rabin, Figure 3A, steps 151A and 152.
[5] Rabin, Figure 3A, step 153.
[6] Rabin, Figure 3B, step 154B.

Although varying in scope and/or directed to a different statutory class, Claims 39 and

41 are similarly amended. Therefore, it is respectfully submitted Claims 37, 39, and 41 (and

any claims depending therefrom) are allowable over the art of record and the outstanding

rejection over 35 U.S.C. § 103(a) should be withdrawn.

Consequently, in view of the present amendment and in light of the above comments,

it is respectfully submitted this application is in condition for allowance. Should the

examiner disagree, the examiner is encouraged to contact the undersigned to discuss any

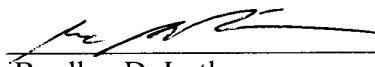remaining issues. Otherwise, an early Notice of Allowance is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, L.L.P.

Customer Number

22850

Tel: (703) 413-3000
Fax: (703) 413-2220
(OSMMN 08/07)

Bradley D. Lytle
Attorney of Record
Registration No. 40,073

Marc A. Robinson
Registration No. 59,276

10